الخليج

اقتصاد, أسواق عالمية

25 أكتوبر 2020 19:43 مساء

نتفليكس» بالعربي أداة تصيّد«

«دبي: «الخليج

اكتشف باحثون في كاسبرسكي موجة من هجمات التصيّد قادتهم إلى موقع ويب خبيث متخفٍّ تمامًا على هيئة صفحة رسمية. ولطالما استغلّ المحتالون منصة «نتفليكس» واستخدموها واجهة خادعة، بوصفها Netflix ««نتفليكس إحدى أشهر منصات البث في العالم، لكن بعضهم فقط يمضي بعيدًا في محاولاتهم الإجرامية عبر إنشاء صفحات للتصيد باللغات المحلية لاستهداف المستخدمين في بلدان ومناطق جغرافية بعينها.

ويُعدّ التصيّد والرسائل الإلكترونية غير المرغوب فيها طرقًا شائعة لشنّ هجمات واسعة النطاق يُستخدم فيها أيضًا في كثير من الأحيان أسماء جهات ومنشآت وعلامات تجارية رسمية، ما يعزز فرص نجاح المحتالين في الحصول على بيانات تسجيل الدخول الخاصة بضحاياهم من المستخدمين. وتمثل الهدف في حالة «نتفليكس» هذه، في استهداف مستخدمي منصة البثّ العالمية.

وأكّدت تاتيانا شيرباكوفا، الباحثة الأمنية في كاسبرسكي، أن المعلومات الشخصية وبيانات الدخول إلى الحسابات

الرقمية باتت في الوقت الحاضر «أكثر المنتجات الرقمية قيمة». وقالت إن بالإمكان تخمين الطرق التي سوف يستغلّ بها المحتالون بيانات الدخول إلى حسابات «نتفليكس» التي يجمعونها بمثل هذه الهجمات، مشيرة إلى كونها مضرة وتخريبية.

وأضافت: «يمكن بيع هذه البيانات عبر الإنترنت المظلمة إذا كان لدى المستخدم اشتراك مسبق الدفع، أو استخدامها لاحقًا لإضفاء المصداقية على المخططات الخبيثة عبر البريد الإلكتروني، مثل الطلب من المستخدمين دفع المال مقابل استعادة الحساب، وحتى الابتزاز. أيضًا، عندما تكون بيانات تسجيل الدخول هي نفسها بيانات تسجيل الدخول إلى حسابات أخرى مهمة، فقد يخترق المجرمون حسابات وسائل التواصل الاجتماعي أو رسائل البريد الإلكتروني، وربما الحسابات المصرفية. ولهذا السبب نوصي دائمًا باستخدام كلمات مرور مختلفة للخدمات المختلفة، واعتماد أسلوب المصادقة الثنائية».

يُذكر أن لدى «نتفليكس» عدداً من الإجراءات المعمول بها لحماية حسابات المستخدمين، بينها صفحة دعم مخصصة تساعد في تحديد الاتصالات المشبوهة والتعامل معها.

هذا، وتوصي كاسبرسكي باتباع الخطوات التالية، لتجنب الوقوع ضحية لمحاولات التصيد التي تتخفّى وراء هيئة منصات شهيرة للبث:

* التحقق دائمًا من عناوين الويب الواردة في الرسائل غير المعروفة أو غير المتوقعة، سواء كان عنوان الويب للموقع الذي يُوجّه إليه المستخدم، أو عنوان الرابط في الرسالة، أو حتى عنوان البريد الإلكتروني للمرسل، من أجل التأكد من أصالتها وأن الرابط في الرسالة الإلكترونية لا يغطي رابطًا آخر.

* تجنّب إدخال بيانات الدخول عند عدم التأكد من كون موقع الويب حقيقيًا. وإذا تمّ ذلك على صفحة مزيفة، ينبغي تغيير كلمة المرور على الفور، كما يجب الاتصال بالبنك أو بأي مزود لخدمات الدفع في حال الشكّ بأن تفاصيل البطاقة قد تعرّضت للاختراق.

.* الحرص على استخدام كلمات مرور قوية ومختلفة لكل حساب، واعتماد أسلوب المصادقة الثنائية